REMARKS/ARGUMENTS

The Examiner rejected claims 1-43 as anticipated (35 U.S.C. §102(e)) by Kuroda (U.S. Patent No. 6,915,434). Applicants traverse for the following reasons.

Applicants amended many of the claims to remove the phrase "capable of" per the request of the Examiner.

During the phone interview, the Examiner clarified that the patent number of Kuroda is 6,915,434, not 6,023,506 as indicated on page 3 of the Third Office Action.

Claims 1, 18, and 27 concern enabling access to data in a storage medium within one of a plurality of storage cartridges capable of being mounted into an interface device and require: providing an association of at least one coding key to the plurality of storage cartridges; encrypting the coding key; and decrypting the encrypted coding key to use to decode and code data stored in the storage medium of the at least one of the storage cartridges.

The Examiner cited FIGs. 1, 2, 11, 13, 16, 22, 23, and 25 and the accompanying text of Kuroda as teaching the claim requirements. If the Examiner maintains the rejection, Applicants request that the Examiner cite to specific sections of the cited references that disclose the independent claim requirements, instead of a general citation to nine figures and their accompanying text which spans several columns of the cited patent. See, 37 CFR 1.104(c)(2) ("When a reference is complex or shows or describes inventions other than that claimed by the applicant, the particular part relied on must be designated as nearly as practicable"); MPEP 707, pg. 700-108, (Rev. 3, Aug. 2005).

Applicants could not identify any part of the cited Kuroda that discloses the claim requirement of encrypting the coding key associated with the storage cartridges and decrypting the coding key to use to decode and code data stored in at least one storage cartridge.

The cited FIG. 1 shows a key management unit 2 and encryption unit 3 for a storage apparatus. (Kuroda, col. 5, lines 33-50) The encrypting unit 3 encrypts data using an individual key stored in the storage apparatus that is unique to the apparatus. The cited FIG. 2 shows a configuration of the storage apparatus that stores three types of keys, an individual key unique to the apparatus, a group key, and a public key used when data is transmitted to another group. (Kuroda, col. 5, line 50 to col. 6, line 9). The cited FIG. 11 is a configuration of the storage apparatus that has a master key storage unit storing a master key which is a common key shared by all apparatuses. (Kuroda, col. 9, lines 35-43) The cited FIG. 13 discusses the how to generate a group key. The cited FIG. 16 shows communication between groups of the storage apparatuses.

(Kuroda, col. 10, line 65 to col. 11, 17). The cited FIG. 22 shows a method for generating a key, including using the group ID to generate a group key. (Kuroda, col. 12, lines 51-67). The cited FIG. 23 shows the generation and distribution of the group key. (Kuroda, col. 13, lines 1-27). The cited FIG. 25 shows how a program is loaded to realize the storage apparatus. (Kuroda, col. 13, line 52 to col. 14, line 10)

The Examiner has not identified any part of the above cited figures and their accompanying text which discloses that the key used to code and decode data written to the storage cartridge is encrypted and decrypted.

During the phone interview, the Examiner specifically referenced step 77 (S77) in the cited FIG. 13, col. 10, lines 1-43 of Kuroda as a point of discussion. This cited col. 10 mentions that to generate a group key, the control unit of the group master obtains group identification information, which is an ID for identifying the group. In step S77, the key management unit selects an individual key stored by the individual key storage unit and the encryption unit generates a group key by encrypting the group identifying information using the individual key. Nowhere does this sited step 77 and FIG. 13 disclose that the key used to code and decode data written to the storage cartridge is encrypted and decrypted. Instead, the cited step 77 discusses how to generate a group key (used to encrypt data transmitted between storage apparatuses) by encrypting group identification information using the individual key.

Moreover, the cited group key is further not used to code and decode data written to the storage, but is instead used to encrypt and decrypt data being transmitted between storage apparatuses. (Kuroda, col. 7, lines 53-65) Nowhere does the cited col. 10 or FIG. 13 disclose or mention encrypting a key used to decode and code data in the storage medium.

If the Examiner maintains the rejection of these claims, Applicants request that the Examiner cite to specific sections of Kuroda that disclose the above independent claim requirements. See, 37 CFR 1.104(c)(2).

Accordingly, for the above reasons, Applicants submit that the independent claims 1, 18, and 27 are patentable over the cited art because the cited Kuroda does not disclose all the claim requirements.

Claims 2-9, 19-22, and 28-35 are patentable over the cited art because they depend from one of claims 1, 18, and 27, which are patentable over the cited art for the reasons discussed above. Moreover, the below discussed independent claims provide additional grounds of patentability over the cited art.

Claims 3, 20, and 29 depend from claims 1, 18, and 27, and further require that the association of the at least one coding key to the plurality of storage cartridges associates one key with the plurality of storage cartridges, wherein the one key is enabled to be used to encode data written to the storage mediums and decode data read from the storage mediums of the plurality of storage cartridges.

Applicants submit that the Examiner has not cited any part of Kuroda that discloses that one key associated with a plurality of storage cartridges is used to encode and decode to the storage mediums of a plurality of storage cartridges. The above discussed Kuroda discusses a group key, but that group key is used to encrypt and decrypt data being transmitted between storage apparatuses. (Kuroda, col. 7, lines 53-65) The cited Kuroda discusses an individual key unique to each storage apparatus used to encrypt and decrypt data on the storage apparatus. However, the Examiner has not cited any part of Kuroda that discloses one key that is used to encrypt and decrypt data written to multiple storage cartridges as claimed. Instead, the cited Kuroda provides a unique individual key for each storage apparatus to encrypt data written to that storage apparatus, not one key to encrypt and decrypt data written to multiple storage apparatuses.

Accordingly, claims 3, 20, and 29 provide additional grounds of patentability over the cited art. If the Examiner maintains the rejection of these claims, Applicants request that the Examiner cite to specific sections of Kuroda that disclose the dependent claim requirements. See, 37 CFR 1.104(c)(2).

Claims 6, 23, and 32 depend from claims 1, 18, and 27 and further require transmitting the encrypted coding key to the interface device, wherein the interface device decrypts the coding key to use to decode and code data stored in the storage medium.

The Examiner cited the sections of Kuroda cited with respect to the independent claims as disclosing the additional requirements of claims 6, 23, and 32. (Third Office Action, pgs. 4-5) Applicants traverse.

The above discussed Kuroda mentions how data is transmitted between storage apparatuses. Applicants submit that the Examiner has not cited any part of Kuroda that discloses transmitting an encrypted coding key to an interface device into which a plurality of storage cartridges can be mounted, where the interface devices decrypts the coding key to decode and code data in the storage medium. Instead, the above discussed Kuroda discusses how storage apparatuses use an individual key to encrypt data to the apparatus and use a group key to encrypt

data transmitted between apparatuses. However, nowhere is there any disclosure of transmitting an encrypted key to an interface device, which decrypts the key and then uses such key to code and decode data.

Accordingly, claims 6, 23, and 32 provide additional grounds of patentability over the cited art. If the Examiner maintains the rejection of these claims, Applicants request that the Examiner cite to specific sections of Kuroda that disclose the dependent claim requirements. See, 37 CFR 1.104(c)(2).

Claims 7-9 and 33-35 include further requirements on encrypting and decrypting the coding key with multiple different keys. Applicant submit that these claims provide further grounds of patentability over the cited art because the Examiner has not cited any part of Kuroda that disclosing encrypting and decrypting the key used to code and decode data in the storage mediums of the cartridges. Accordingly, the additional requirements of these claims concerning using multiple keys to encrypt and decrypt the key provides further grounds of patentability over the cited art. If the Examiner maintains the rejection of these claims, Applicants request that the Examiner cite to specific sections of Kuroda that disclose the dependent claim requirements. See, 37 CFR 1.104(c)(2).

Independent claims 10, 23, and 36 concern an interface device for accessing data in a removable storage cartridge including a storage medium coupled to the interface device and require: receiving an encrypted coding key from a host system; decrypting the encrypted coding key; using the coding key to encode data to write to the storage medium; and using the coding key to decode data written to the storage medium.

The Examiner cited the same above cited paragraphs of Kuroda as disclosing the additional requirements of these claims. (Third Office Action, pg. 6) Applicants traverse.

The above discussed Kuroda discusses how each storage apparatus has an individual key to encrypt data to the apparatus and uses a group or public key to encrypt data for transfer to another storage apparatus. The Examiner has not cited any part of Kuroda that discloses that an interface device to which removable cartridges are coupled receives an encrypted coding key from a host system, decrypts the key and uses the key to code and decode data in a removable storage cartridge. Instead, the above cited Kuroda discusses how storage apparatuses use keys to encrypt data written to the storage or transmitted.

Accordingly, for the above reasons, Applicants submit that the amended independent claims 10, 23, and 36 are patentable over the cited art because the cited Kuroda does not disclose all the claim requirements.

Claims 11-17, 24-26, and 37-43 are patentable over the cited art because they depend from claims 10, 23, and 36, which are patentable over the cited art for the reasons discussed above. Moreover, the dependent claims provide additional details about how the coding key may be encrypted and decrypted. The cited Kuroda does not disclose the additional requirements of the dependent claims with respect to how a key is encrypted and decrypted because the Examiner has not cited where Kuroda discloses that the storage apparatuses encrypt and decrypt their individual keys. Accordingly, these dependent claims provide further grounds of patentability over the cited art.

For instance, claims 15, 26, and 41 depend from claims 12, 24, and 38 and further require storing the coding key encrypted with the first key within the storage cartridge; receiving an input/output (I/O) request directed to the storage cartridge; and accessing the encrypted coding key from the storage cartridge, wherein the accessed coding key is decrypted using the second key, and wherein the decrypted coding key is used to encode and decode data to execute the I/O request to the storage cartridge.

The Examiner has not cited any part of Kuroda that disclose that in response to an I/O request, the encrypted coding key is accessed from the storage cartridge and decrypted using a second key, and using the decrypted coding key to execute the I/O request.

As discussed, the cited Kuroda discusses how storage apparatuses use individual keys to encrypt data in their apparatus. However, The Examiner has not cited where Kuroda discloses that this encrypted coding key is received from a host system and accessed from the storage key and decrypted using a second key in order to use the decrypted coding key to execute the I/O request.

Conclusion

For all the above reasons, Applicant submits that the pending claims 1-43 are patentable over the art of record. Applicants have not added any claims. Nonetheless, should any additional fees be required, please charge Deposit Account No. 09-0466.

The attorney of record invites the Examiner to contact him at (310) 553-7977 if the Examiner believes such contact would advance the prosecution of the case.

Dated: February 8, 2006

By:_____

David W. Victor
Registration No. 39,867

Please direct all correspondences to:

David Victor
Konrad Raynes & Victor, LLP
315 South Beverly Drive, Ste. 210
Beverly Hills, CA 90212
Tel: 310-553-7977
Fax: 310-556-7984